

Clear Desk and Clear Screen Policy

Version	Approval Date	Owner
1.0	December 1, 2018	Privacy Officer

1. Purpose

The purpose of this policy is to ensure confidential data is kept private and protected from unauthorized access and viewing. The goal is to reduce the risks of unauthorized access to, or loss of, or damage to, HealthShare Exchange (HSX) enterprise data.

2. Scope

This policy applies to all HSX confidential data, computing devices, and employees, interns, consultants and contractors.

3. Policy

Clear Desk and Clear Screen Policy

- HSX shall develop and adopt a clear desk policy for confidential data, including paper media and removable media, and a clear screen policy for information assets in order to reasonably limit uses and disclosures to the minimum necessary. The policy shall be communicated to all employees, interns, consultants and contractors.
- Confidential data on paper media or in removable media shall not be left unattended.
- Confidential data on paper media shall be protected from access by unauthorized individuals when not in use by storing in a locked drawer or cabinet.
- Confidential data in removable media shall be protected from access by unauthorized individuals when not in use according to the *Encryption Policy*.
- Confidential data on paper media shall be immediately removed from printers, copiers, or fax machines to prevent access by unauthorized individuals.
- Reproduction technology (e.g., printers, copiers, scanners, cameras, facsimile machines, etc.) shall be protected both physically and logically from use by unauthorized individuals to prevent unauthorized reproduction of confidential data.



- Passwords shall not be posted on, under, or near a computer or other computing device according to the *Acceptable Use Policy*.
- Incoming and outgoing distribution points for inter-office mail shall be protected from physical access by unauthorized individuals so that mail cannot be stolen or lost.
- Confidential data that has been copied or printed shall be protected during transport using internal or external (e.g., USPS) mail services. This includes ensuring non-address information is not visible through envelope windows and marking the envelopes according to the *Data Classification and Data Handling, Labeling, and Storage Policies*.
- All employees and contractors shall close all applications, logout, or lock their computer when they are away from their desk to protect confidential data from unauthorized access and viewing.
- All employees and contractors shall logout of each application and log off the network when they leave their work stations at the end of the workday to protect confidential data from unauthorized access and viewing.
- All computer screen savers should be set for a maximum of twenty minutes to lock requiring a password to reenter the computer.

4. Procedure

None

5. Enforcement

The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the President

6. Definitions

For a complete list of definitions, refer to the *Glossary*.

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.310(b), HIPAA § 164.312(a)(2)(i)
- HITRUST Reference: 01.h Clear Desk and Clear Screen Policy



HealthShare Exchange

1801 Market Street, Suite 750 Philadelphia PA, 19103 www.healthshareexchange.org

Policy Owner	Privacy Officer	Contact	Don.Reed@healthshareexchange.org
Approved By	Board HSX Management Team	Approval Date	December 1, 2018
Date Policy In Effect	May 26, 2015	Version #	1.0
Original Issue Date	May 26, 2015	Last Review Date	September 17, 2020 December 1, 2018
Related Documents	Acceptable Use Policy Data Classification Policy Data Handling, Labeling, and Storage Policy Encryption Policy Glossary		